|  |  |
| --- | --- |
| 114.A: General Data Protection Regulation (GDPR) Policy | |
| Version: 1 | Effective Date: March 6, 2019 |

Human subjects research conducted at Illinois State University will comply with the provisions of the General Data Protection Regulation (GDPR), which established protections on “personal data” from individuals physically located in the European Economic Area (EEA) at the time of data-collection.

The **European Economic Area (EEA)** consists of:

* Austria
* Belgium
* Bulgaria
* Croatia
* Republic of Cyprus
* Czech Republic
* Denmark
* Estonia
* Finland
* France
* Germany
* Greece
* Hungary
* Iceland
* Ireland
* Italy
* Latvia
* Lichtenstein
* Lithuania
* Luxembourg
* Malta
* Netherlands
* Norway
* Poland
* Portugal
* Romania
* Slovakia
* Slovenia
* Spain
* Sweden
* UK

This policy applies to any study that has the potential of collecting or obtaining personal identifiable information from one or more research participants that are physically located in the European Economic Area (EEA), whether the participant is a citizen of an EEA country or not. “Personal data” includes any information that relates to an identified or identifiable natural person (i.e., an individual, not a company or other legal entity), otherwise known as a “data subject.”

Examples of personal data include:

* + name and surname;
  + home address;
  + email address such as [name.surname@company.com](mailto:name.surname@company.com);
  + identification card number;
  + location data (for example the location data function on a mobile phone)\*;
  + Internet Protocol (IP) address;
  + cookie ID\*;
  + advertising identifier of the participant’s phone;
  + data held by a hospital or doctor, which could uniquely identify a person.

GDPR also applies to data elements that, in combination, could reveal personally identifiable information about the individual.

The GDPR ***does not apply*** to anonymous data. It also does not apply to deidentified data if the researcher had no role in collecting the originally identifiable data. . “Pseudonymized data” (e.g., coded data) is considered to be “personal data” if a key exists.

**Rights of Data Subjects**

An individual has several rights under the GDPR including the right to:

* **information** about the processing of personal data;
* **obtain access to** the personal data held about the individual;
* **Ask** for incorrect, inaccurate or incomplete personal data to be **corrected**;
* Request that personal **data be erased** when it’s no longer needed or if processing it is unlawful;
* **Object** to the processing of the individual’s personal data for marketing purposes or on grounds relating to your particular situation;
* Request the **restriction** of the processing of personal data in specific cases;
* Receive personal data in a machine-readable format and send it to another controller (‘**data portability**’);
* Request that decisions based on **automated processing** concerning the individual or significantly affecting the individual are made by natural persons, not only by computers.

In order for any person that may have GDPR rights to exercise the rights, the individual you should contact the University’s Data Protection Officer, Kevin Crouse at 309-438-5533 or via email at [kcrouse@ilstu.edu](mailto:kcrouse@ilstu.edu). The University will respond to requests without undue delay and **at the latest within 1 month.** If, for some reason, the University cannot comply with a request, the University will provide a reason why in writing.

**Approval Criteria**

In addition to meeting all regulations pertaining to human subjects research conducted in the U.S., studies that are subject to the GDPR must conform to approval criteria and provide informed consent provisions required in the law. The additional approval criteria include:

1. The minimum necessary amount of identifiable data is collected to conduct the research.
2. Data security provisions are appropriate for the level of sensitivity as determined by the Data Protection Officer. Any third-party website or other third party or app being used for data collection should be GDPR-compliant as a Data Processor, as that term is defined under the GDPR. Use of any third-party website or app not on the [approved list (Appendix A)](#list), must be approved by the Data Protection Officer ([informationsecurityoffice@ilstu.edu](mailto:informationsecurityoffice@ilstu.edu)). Approval from the IRB does not indicate that approval from the Data Protection Officer has been granted.
3. The consent process includes both the Letter of Information and the Consent Document and both conform to the requirements listed in the Consent section of this policy. An executable plan to remove data in the event a participant requests to have their data removed must be in place and described in the protocol. Data that has been deidentified before the request is made does not need to be removed.

**Data Security and Sharing**

The GDPR requires that technical and organizational security measures appropriate to the risk to the subject’s Personal Data are implemented.

**Data sharing** under the GDPR is allowed only if:

1. The subject actively consents to the future use. Risks of transfer must be fully described in the consent documents.
2. The data is anonymized when possible.
3. If data are not anonymized, establish a robust system for tracking with whom data are shared in the event that participants request that their data be deleted, and inform these researchers that the data are subject to the GDPR.

Any **data breach** occurring on a project involving GDPR-covered data must be reported **within 72 hour**s upon identification of the breach to the Data Protection Officer, Kevin Crouse (309) 438-5533 or [informationsecurityoffice@ilstu.edu](mailto:informationsecurityoffice@ilstu.edu)). An adverse event submission will also need to be submitted in Cayuse IRB describing the breach.

[**GDPR**](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#abouttheregulationanddataprotection) **Consent Criteria**

. In addition to U.S. regulations and ISU policy, under the GDPR consent must be;

1. Freely given. – there must be a realistic choice or the ability to refuse or withdraw consent without detriment.
2. Specific – each purpose and rights must be specifically stated in the consent, including any future use of the data.
3. Informed – the nature and extent to which the data will be used, how long the data will be retained, and how it will be collected.
4. Unambiguous – consent must be given as a clear affirmative act. Passive consent is not allowed.

The GDPR consent process requires two steps – a Letter of Information as one document and a Consent Document as a separate document.

1. Letter of Information

The letter of information mirrors the standard consent forms but without the signatures and with additional elements. The letter must have separate sections with section headings.

Standard elements:

* A statement that the study involves research
* An explanation of the purposes of the research
* The expected duration of the subject's participation
* A description of the procedures to be followed
* Identification of any procedures which are experimental
* A description of any reasonably foreseeable risks or discomforts to the subject
* A description of any benefits to the subject or to others which may reasonably be expected from the research
* A disclosure of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to the subject
* A statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained
* For research involving more than minimal risk, an explanation as to whether any compensation, and an explanation as to whether any medical treatments are available, if injury occurs and, if so, what they consist of, or where further information may be obtained
* An explanation of whom to contact for answers to pertinent questions about the research and research subjects' rights, and whom to contact in the event of a research-related injury to the subject
* A statement that participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and the subject may discontinue participation at any time without penalty or loss of benefits, to which the subject is otherwise entitled
* A statement that significant new findings developed during the course of the research, which may relate to the subject's willingness to continue participation, will be provided to the subject
* The approximate number of subjects involved in the study

Additional Elements Required by the GDPR:

* Whether and under what conditions participant data may be used for future research, either related or unrelated to the purpose of the current study must be included.
* Sensitive data must be specifically listed:
  + Racial or ethnic origin
  + Political opinions
  + Religious or philosophical beliefs
  + Trade union membership
  + Processing of genetic data
  + Biometric data for the purposes of unique identification
  + Health data
  + Sexual orientation information
  + Data concerning a natural person’s sex life.
* Information regarding automated processing of data for decision-making about the individual, including using automated programs to profile individuals or place participants into certain conditions based upon their responses.
* Detailed Information regarding data security, including storage and transfer of data must be included.
* How long identifiable participant data will be stored (this can be indefinite)
* A detailed description of the data processing and transfer activities to be performed, if applicable. This includes describing any software used to process information and what methods will be used to transfer data such as transferring recordings from recording device to a private computer.
* Right to withdraw and the mechanism for withdrawal. Withdrawal of consent must be as easy as giving consent.
* Right to erasure. Under certain circumstances, individuals have the right to ask for their personal data to be deleted.

1. Consent Document

The consent document includes all of the specific elements of the study that are described in the Letter of Information. The elements are presented as a list with a box next to each element where the participant will mark or initial the box next to the element to indicate consent. To conform to the “clear requirement that the boxes cannot be pre-checked.

1. Waivers of Consent/Documentation of Consent

Waivers of consent are not acceptable under the GDPR. Waivers of documentation are not acceptable with the exception of exemptable studies where the participant could check an “I agree” box to substitute for a written signature.

1. Data Collection from Children

Under the GDPR, data collection from anyone under the age of 16 requires explicit consent of the “holder of parental responsibility.” Individual EEA countries may lower that age, but the minimum age is 13. This requirement supersedes the parental permission/child assent provisions applicable to non-GDPR research.

**Alternatives for Researchers**

For researchers who are conducting survey research but do not seek responses from individuals in the EEA, the following options are available:

1. Include a statement in the consent form that subjects present in the EEA are not eligible to participate.
2. Include a checkbox for the participant to actively affirm that they are not in the EEA when completing the survey.

**Appendix A: List of Third Party Websites and Apps determined to be GDPR Complaint**

\*\*This list will be updated periodically\*\*

1. Qualtrics
2. Zoom